REMARKS

The Applicants thank the Examiner for granting an interview on June 21, 2007. In accordance with the foregoing, independent claims 1, 28 and 36 are amended for clarity and to improve form, as discussed in the interview. It is understood, according to the Interview Summary, the next Office Action will not be final.

STATUS OF THE CLAIMS:

Claims 1-38 have been pending.

It is understood that claims 7, 13-16 and 18-27, 29-33, 35 and 37-38 are withdrawn from consideration.

According to the Examiner, claims 1, 2, 5, 6, 8-12, 17, 28 and 36 are the elected pending claims, but it is submitted that claims 34 is also constructively elected as set forth below.

In accordance with the foregoing, the claims are amended, and, thus, the elected pending claims remain for reconsideration, which is respectfully requested.

No new matter has been added.

The Examiner's rejections are respectfully traversed.

WITHDRAWN CLAIMS

The Office Action Summary indicated claims 1, 2, 5, 6, 8-12, 17, 28 and 36 are pending. However, claims 1-38 are pending and claims 1, 2, 5, 6, 8-12, 17, 28, 34 and 36 are elected and claims 7, 13-16 and 18-27, 29-33, 35 and 37-38 are withdrawn. Correction of the Office Action is respectfully requested. Applicants elected independent claim 34 (group I) in the response to the restriction requirement filed April 20, 2006.

Independent claim 34 should be joined with elected pending claims for being a generic claim by reciting "A computer-readable storage medium storing a method executed by a central processing unit for decrypting ~~on which is recorded~~ a program code ~~executed by a computer, wherein~~ according to operations comprising:~~the program code is encrypted with a code encryption key;~~ entering a license into the central processing unit before the program code is executed, wherein ~~a~~ the license, which includes ~~the~~ a code encryption key, ~~and~~ is encrypted with a public key which is ~~paring~~ paired with a private key ~~comprised in secrecy~~hidden within ~~a~~ the central processing unit ~~comprised by the computer to execute the program code,~~ and is provided in correspondence with the program code; ~~the license is entered into the central~~

~~processing unit before the program code is executed;~~decrypting the license is ~~decrypted~~ with the private key ~~by~~ with the central processing unit; and decrypting the program code ~~is decrypted~~ with the code encryption key obtained from the license ~~by~~ with the central processing unit."

The previous Office Action, mailed July 13, 2006, at the Office Action Summary asserts claim 34 is withdrawn. However, the Office Action mailed March 23, 2006, at page 4, item 10 states "Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. **Currently claim 1, 2, 28, 34 and 36 are generic**" (emphasis added).

MPEP §803 recites "If the search and examination of **>all the claims in an< application can be made without serious burden, the examiner must examine *>them< on the merits, even though **>they include< claims to independent or distinct inventions." The Examiner did not include claim 34 as a species in the Restriction Requirement and indicated that claim 34 is generic. Therefore the Applicants respectfully submit it should not be a serious burden on the Examiner to examine claim 34.

Correction of the Office Action is respectfully requested.

CLAIM REJECTIONS:

Claims 1, 2, 5, 6, 8-12, 17, 28 and 36 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hashimoto et al., U.S. Patent Publication 2001/0018736, hereinafter referred to as "Hashimoto."

In accordance with the foregoing, independent claims 1, 28 and 36 are amended for clarity and to improve form, as discussed in the interview. Claim 1, for example, is amended to recite:

> A central processing unit ~~executing a program~~, comprising:
>
> a first private key concealed in secrecy;
>
> an encrypting unit obtaining, from a first license of a first program, an access condition for accessing a memory region during an execution process of the first program and a code decryption key for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first license of the first program encrypted with a public key pairing with the first private key~~encrypting a block and decrypting an encrypted block~~; ~~and~~
>
> a tamper resistant buffer that a user cannot reference or falsify~~,~~;
>
> a Translation Lookaside Buffer (TLB) linked to said tamper

resistant buffer and recording an address of the memory region, at which the encrypted block which configures the first program is recorded, and recording the access condition to the memory region obtained from the license;

a memory managing unit; and

a processor core, wherein:

...

the code decryption key obtained from said license of the first program is recorded to said tamper resistant buffer,

...

~~wherein~~ said memory managing unit obtains the access condition to the memory region at which the encrypted block is recorded from said TLB based on an address ~~or a~~of the memory region~~, at which an encrypted block is recorded,~~ and further obtains the code decryption key corresponding to the memory region from said tamper resistant buffer, and

~~wherein~~ said processor core ~~determines whether~~ permits an access to the memory region ~~is permitted to be made~~ from the execution process of the first program based on the access condition obtained by said memory managing unit....

The Office Action, at item 4, asserts that Hashimoto at paragraphs 74 and 75 discloses the claimed "encrypting unit obtaining, from a first license of a first program, an access condition for accessing a memory region during an execution process of the first program and a code decryption key for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first license of the first program encrypted with a public key pairing with the first private key," as recited, for example, in claim 1. Applicants respectfully disagree with the assertion, because Hashimoto at paragraphs 72-75, merely provides:

The object of this embodiment is to protect the program instructions (execution codes) and the execution state from a user of the target system who can freely read the main memory of the target system and freely alter the OS program or application programs.

The basic features for achieving this object are the access control with respect to the information storage inside the processor and the encryption based on the information listed below.

(1) A common key Kx selected by a program creator. The application program will be encrypted by the secret key cryptosystem using this key.

(2) A pair of a unique public key Kp and a unique secret key Ks provided inside the processor. The public key can be read out by the program by using instructions.

In other words, Hashimoto at paragraphs 72 to 75 merely discusses that a common key Kx, a public key Kp and a secret key Ks are used to encrypt execution codes. Furthermore, Hashimoto discusses, in the abstract:

> **a tamper resistant microprocessor saves a context information for one program whose execution is to be interrupted, where the context information contains information indicating an execution state of that one program and the execution code encryption key of that one program.** An execution of that one program can be restarted by recovering the execution state of that one program from the saved context information. The context information can be encrypted by using the public key of the microprocessor, and then decrypted by using the secret key of the microprocessor.

Furthermore, Hashimoto discusses, at paragraph 150:

> In the case of interrupting the execution of some program, the context information encryption/decryption unit 254 of **the exception processing unit 131 encrypts information indicating the execution state up to an interrupted point of the program to be interrupted** and the code encryption key of this program by using the public key of the microprocessor 101, and writes the encrypted information into the main memory 281 as the context information.

In other words, Hashimoto discusses restoring a program whose execution is interrupted by a tamper by encrypting the execution codes using the common key Kx, the public key Kp and the secret key Ks.

In contrast, the claimed embodiment provides, in part, "an encrypting unit obtaining, from a first license of a first program, an access condition for accessing a memory region during an execution process of the first program and a code decryption key for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first license of the first program encrypted with a public key pairing with the first private key," as recited, for example, in claim 1. Hashimoto fails to disclose, either expressly or implicitly, the claimed "encrypting unit," because Hashimoto is merely related to restoring a program, whose execution is interrupted by a tamper, after encrypting the execution codes, and, thus fails to disclose, either expressly or implicitly, encrypting/decrypting any program configuration. Furthermore, Hashimoto fails to disclose, either expressly or implicitly, the claimed "obtaining, **from a first license of a first program, an access condition** for accessing a memory region during an execution process of the first program **and a code decryption** key for decrypting an encrypted

block configuring the first program, by decrypting with the first private key the first license of the first program encrypted with a public key pairing with the first private key."

Furthermore, the Office Action at page 3, lines 2-3, fails to cite any reference against the claimed "first license." Applicants respectfully submit that Hashimoto fails to disclose the claimed "first license" including "an access condition," because Hashimoto is related to restoring a program, whose execution is interrupted by a tamper, after encrypting the execution codes, and, thus, fails to disclose, either expressly or implicitly, any "license" or any "access condition."

The Office Action, at page 3, asserts that Hashimoto at paragraph 146 discloses the claimed "Translation Lookaside Buffer (TLB) linked to said tamper resistant buffer and recording an address of the memory region, at which **the encrypted block which configures the first program** is recorded, **and recording the access condition to the memory region** obtained from the license." Applicants respectfully disagree, because Hashimoto at paragraph 146 merely discusses:

> The exception processing unit 131 further includes a register file 253, a context information encryption/decryption unit 254, an exception processing unit 255, a secret protection violation detection unit 256, and an execution code encryption key and signature verification unit 257.

Applicants respectfully submit that Hashimoto fails to disclose, either expressly or implicitly, the claimed "Translation Lookaside Buffer (TLB) linked to said tamper resistant buffer and recording an address of the memory region, at which **the encrypted block which configures the first program** is recorded, **and recording the access condition to the memory region** obtained from the license," as recited, for example, in claim 1, because, as discussed above, Hashimoto fails to disclose, either expressly or implicitly, the claimed "encrypting unit obtaining, from a first license of a first program, an access condition for accessing a memory region during an execution process of the first program and a code decryption key for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first license of the first program encrypted with a public key pairing with the first private key."

The Office Action, at page 3, asserts that Hashimoto, at paragraph 247, discloses the claimed "processor core ~~determines whether~~ permits an access to the memory region ~~is permitted to be made~~ from the execution process of the first program **based on the access condition obtained by said memory managing unit**," as recited, for example, in claim 1. Applicants respectfully disagree, because Hashimoto, at paragraphs 245-247, merely discusses:

> In this embodiment, the encryption attributes for protecting data are defined in four registers CY0 to CY3 that are provided inside the microprocessor 101. They correspond to regions 717 to 720 shown in FIG. 9. In FIG. 9, details of the registers CY0 to CY2 are omitted, and only details of the register CY3 are shown.
>
> ...
>
> Among the specifications of the regions, CY0 is given the highest priority, and CY1 to CY3 are given sequentially lower priorities in this order. For example, when the regions specified by CY0 and CY1 overlap, the attributes of CY0 are given the priority over those of CY1 in that region. Also, the definition of the page table is given the highest priority in the case of a memory access as the execution code rather than as the processing target data.

In other words, Hashimoto discusses that a register CY0 is given a higher priority than registers CY1 to CY3. However, Hashimoto fails to disclose, either expressly or implicitly, the claimed "processor core ~~determines whether~~ permits an access to the memory region ~~is permitted to be made~~ from the execution process of the first program based on the access condition obtained by said memory managing unit," as recited, for example, in claim 1, because, as discussed above, Hashimoto fails to disclose, either expressly or implicitly, a "first license" including an "access condition."

Thus, a prima facie case obviousness based upon Hashimoto cannot be established, because Hashimoto discusses restoring a program whose execution is interrupted by a tamper by encrypting the execution codes which fails to provide any motivation or suggestion to one skilled in the art to modify Hashimoto to achieve the claimed central processing unit comprising "a first private key concealed in secrecy; an encrypting unit obtaining, from a first license of a first program, an access condition for accessing a memory region during an execution process of the first program and a code decryption key for decrypting an encrypted block configuring the first program, by decrypting with the first private key the first license of the first program encrypted with a public key pairing with the first private key~~encrypting a block and decrypting an encrypted block~~; ~~and~~ a tamper resistant buffer that a user cannot reference or falsify~~,~~; a Translation Lookaside Buffer (TLB) linked to said tamper resistant buffer and recording an address of the memory region, at which the encrypted block which configures the first program is recorded, and recording the access condition to the memory region obtained from the license; a memory managing unit; and a processor core, wherein: ... the code decryption key obtained from said license of the first program is recorded to said tamper resistant buffer, ... ~~wherein~~ said memory managing unit obtains the access condition to the memory region at which the encrypted block is

recorded from said TLB based on an address ~~or a~~of the memory region~~, at which an encrypted block is recorded,~~ and further obtains the code decryption key corresponding to the memory region from said tamper resistant buffer, and ~~wherein~~ said processor core ~~determines whether~~ permits an access to the memory region ~~is permitted to be made~~ from the execution process of the first program based on the access condition obtained by said memory managing unit," as recited, for example, in claim 1.

Independent claims 28 and 36 patentably distinguish over the cited prior art for similar reasons as independent claim 1.

Dependent claims recite patentably distinguishing features of their own or are at least patentably distinguishing due to their dependence from the independent claims. Withdrawal of the rejection of pending claims, and allowance of pending claims is respectfully requested.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: July 9, 2007

By: _____

Matthew H. Polson
Registration No. 58,841

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501